CONGRESSIONAL BUDGET OFFICE
COST ESTIMATE

October 31, 2011

S. 1408
Data Breach Notification Act of 2011

As ordered reported by the Senate Committee on the Judiciary on September 22, 2011

SUMMARY

S. 1408 would require most federal agencies and business entities that collect, transmit, store, or use sensitive personal information to notify any individuals whose information has been unlawfully accessed through a breach in security systems designed to protect such information from unauthorized access. The legislation defines sensitive personal information as combinations of an individual's name, address or phone number, and Social Security number, driver's license number, financial account information, or biometric data (that is, finger print, voice print, or retina scan). Under certain circumstances, entities could apply to the federal government for exemptions from those notification requirements. In addition, the affected entities would be required to notify the Department of Homeland Security (DHS) and the Federal Trade Commission (FTC) of a security breach. Finally, S. 1408 would impose civil penalties on entities that fail to provide notice to affected individuals.

CBO estimates that, assuming appropriation of the necessary amounts, implementing the bill would cost about $15 million over the 2012-2016 period. Enacting the bill also could affect direct spending and revenues; therefore, pay-as-you-go procedures apply. However, any such effects would not be significant.

S. 1408 contains intergovernmental and private-sector mandates, as defined in the Unfunded Mandates Reform Act (UMRA), but CBO estimates the costs to comply with those mandates would not exceed the thresholds in that act ($71 million and $142 million, respectively, in 2011, adjusted annually for inflation).

ESTIMATED COST TO THE FEDERAL GOVERNMENT

Assuming appropriation of the necessary amounts, CBO estimates that implementing S. 1408 would cost about $3 million annually for the FTC and federal law enforcement agencies to specify how the required notification procedures would work. CBO expects

that most government agencies would incur negligible costs to implement the legislation because they already comply with notification requirements similar to those in the bill.

Enacting the legislation could increase collections of civil penalties (which are recorded in the budget as revenues) and could affect direct spending by agencies not funded through annual appropriations. CBO estimates, however, that any changes in revenues and net spending would be negligible.

PAY-AS-YOU-GO CONSIDERATIONS

The Statutory Pay-As-You-Go Act of 2010 establishes budget-reporting and enforcement procedures for legislation affecting direct spending or revenues. CBO estimates that enacting S. 1408 would have a negligible effect on direct spending and revenues.

ESTIMATED IMPACT ON STATE, LOCAL, AND TRIBAL GOVERNMENTS

S. 1408 contains intergovernmental mandates as defined in UMRA because it would explicitly preempt laws in at least 46 states that require businesses to notify individuals in the event of a security breach and would impose notification requirements and limitations on state Attorneys General. Because the limits on state authority would impose no duties with costs and because the notification requirements would result in minimal additional spending, CBO estimates the costs of the mandates would be small and would not exceed the threshold established in UMRA for intergovernmental mandates ($71 million in 2011, adjusted annually for inflation).

ESTIMATED IMPACT ON THE PRIVATE SECTOR

S. 1408 would impose private-sector mandates as defined in UMRA on business entities that handle sensitive personal information and on credit reporting agencies. Because most of those businesses already comply with similar requirements in state laws, CBO estimates that the incremental cost to comply with the mandates in the bill would probably fall below the annual threshold established in UMRA for private-sector mandates ($142 million in 2011, adjusted annually for inflation).

Notification of Security Breaches

The bill would require business entities engaged in interstate commerce that use, access, transmit, store, dispose of, or collect sensitive personally identifiable information (PII) to notify any individuals whose information has been or may have been unlawfully accessed as result of a breach. Entities would be able to notify individuals using written letters, the

telephone, or email under certain circumstances. If a business entity does not own or license the breached information, the business would have to notify the owner or licensee of the information following a breach.

In the event of a large security breach, entities would be required to take steps to notify the general public as well as certain federal agencies. For instance, if an entity experiences a breach that compromises the PII of more than 5,000 individuals, that entity would be required to notify individuals affected, consumer reporting agencies, and major media outlets serving the state or jurisdiction where the breach occurred. If the breach involves more than 10,000 individuals, several federal agencies also would have to be notified. The bill, however, would exempt business entities from the notification requirements under certain circumstances.

According to industry sources, millions of individuals' sensitive personally identifiable information is breached every year. However, according to those sources, at least 46 states already have laws requiring notification in the event of a security breach. In addition, it is the standard practice of most business entities to notify individuals if a security breach occurs. Therefore, CBO estimates that the incremental costs incurred by businesses to comply with the notification requirements in the bill would probably fall below the annual threshold for private-sector mandates.

Fraud Alert

The bill also would require consumer reporting agencies to include an extended fraud alert in a consumer's file if that consumer submits evidence that they have received notice that the consumer's financial information has or may have been compromised. Under current federal law, consumer reporting agencies are required to provide an extended fraud alert service if a consumer submits an identity theft report and a temporary fraud alert if requested by a consumer in good faith. The current industry practice is to provide extended alerts for any consumer who can present evidence that their personal information may have been compromised, without submitting an identity theft report. Several state laws also require the practice. The cost of the mandate would be the incremental cost for consumer reporting agencies to include additional extended fraud alerts in consumers' files. Based on information from industry sources, CBO estimates that the incremental cost to comply with this mandate would be minimal.

PREVIOUS CBO ESTIMATE

On October 27, 2011, CBO transmitted a cost estimate for S. 1151, the Personal Data Privacy and Security Act of 2011, as ordered reported by the Senate Committee on the Judiciary on September 27, 2011. The two pieces of legislation have different provisions but are similar because they deal with unauthorized access to personal information; as a

result, the estimated costs are similar: about $3 million per year for implementation, subject to appropriation of the necessary amounts.

ESTIMATE PREPARED BY:

Federal Costs: Mark Grabowicz, Matthew Pickford, Jason Wheelock, and Susan Willie
Impact on State, Local, and Tribal Governments: Elizabeth Cove Delisle
Impact on the Private Sector: Marin Randall

ESTIMATE APPROVED BY:

Theresa Gullo
Deputy Assistant Director for Budget Analysis